CERT Advisory CA-2002-22 Multiple Vulnerabilities in Microsoft SQL Server

Original release date: July 29, 2002
Last revised: February 5, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000
- Any application that includes MSDE

Overview

The Microsoft SQL Server contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts. These vulnerabilities are public and have been addressed by Microsoft Security Bulletins, but we believe their collective severity warrants additional attention.

I. Description

Since December 2001, Microsoft has published eight Microsoft Security Bulletins regarding more than a dozen vulnerabilities in the Microsoft SQL Server. This document provides information on the five most serious of these vulnerabilities; references to the remainder are provided in Appendix B.

In isolation, many of these vulnerabilities have significant preconditions that are difficult for an attacker to overcome. However, when exploited in combination, they allow attackers to gain additional flexibility and increase their chances for success. In particular, the privilege escalation vulnerability described in VU#796313 allows an attacker to weaken the security policy of the SQL server by granting it the same privileges as the operating system. With full administrative privileges, a compromised Microsoft SQL Server can be used to take control of the server host.

The CERT/CC encourages system administrators to take this opportunity to review the security of their Microsoft SQL servers and to apply the appropriate patches from the Microsoft bulletins listed in Appendix B.

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges (CAN-2002-0642)

> *The Microsoft SQL Server typically runs under a dedicated "service account" that is defined by system administrators at installation time. This definition is stored in the Windows registry with permissions that allow the SQL Server to change the value of the registry key. As a result, attackers with access to the "xp_regwrite" extended stored procedure can alter this registry key and cause the SQL Server to use the LocalSystem account as its service account.*
>
> *Upon rebooting the server host or restarting the SQL service, the SQL Server will run with the full administrative privileges of the LocalSystem account. This ability allows a remote attacker to submit SQL queries that can execute any command on the system with the privileges of the operating system.*

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function
(CAN-2002-0624)

> *The Microsoft SQL Server provides multiple methods for users to authenticate to SQL databases. When SQL Server Authentication is used, the username and password of each database user is stored in a database on the SQL server. When users supply a password to the server using this method, a function named pwdencrypt() is responsible for encrypting the user-supplied password so that it can be compared to the encrypted password stored on the SQL server.*
>
> *There is a buffer overflow in pwdencrypt() that allows remote attackers to execute arbitrary code on the SQL server by supplying a crafted password value. Successful exploitation of this vulnerability requires knowledge of a valid username and will cause the supplied code to execute with the privileges of the SQL service account.*

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows
(CAN-2002-0154)

> *Microsoft SQL Server provides a scripting construct known as an "extended stored procedure" that can execute a collection of server commands together. Several of the extended stored procedures included with the Microsoft SQL Server contain buffer overflow vulnerabilities. These procedures provide increased functionality for database applications, allowing them to access operating system or network resources.*

> *Parameters are passed to extended stored procedures via an API that specifies the actual and maximum length of various parameter data types. Some of the extended stored procedures fail to adequately validate the length of input parameters, resulting in stack buffer overflow conditions.*
>
> *Since some of the vulnerable procedures are configured by default to allow public access, it is possible for an unauthenticated attacker to exploit one or more of these buffer overflows. SQL Server databases are commonly used in web applications, so the vulnerable procedures may be accessible via the Internet. Microsoft Security Bulletin MS02-020 states*
>
> > *An attacker could exploit this vulnerability in one of two ways. Firstly, the attacker could attempt to load and execute a database query that calls one of the affected functions. Secondly, if a web-site or other database front-end were configured to access and process arbitrary queries, it could be possible for the attacker to provide inputs that would cause the query to call one of the functions in question with the appropriate malformed parameters.*

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service
(CAN-2002-0649)

> *The SQL Server Resolution Service (SSRS) was introduced in Microsoft SQL Server 2000 to provide referral services for multiple server instances running on the same machine. The service listens for requests on UDP port 1434 and returns the IP address and port number of the SQL server instance that provides access to the requested database.*
>
> *The SSRS contains a heap buffer overflow that allows unauthenticated remote attackers to execute arbitrary code by sending a crafted request to port 1434/udp. The code within such a request will be executed by the server host with the privileges of the SQL Server service account.*

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service
(CAN-2002-0649)

> *The SSRS also contains a stack buffer overflow that allows unauthenticated remote attackers to execute arbitrary code by sending a crafted request to port 1434/udp. The code within such a request will be executed by the server host with the privileges of the SQL Server service account.*

II. Impact

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

> *As a precondition, this vulnerability requires the ability to modify the SQL service account registry key (for example, via the "xp_regwrite" extended stored procedure). Attackers must convince an administrator to grant this access, or they must obtain it by exploiting one of the vulnerabilities listed in this advisory.*
>
> *This vulnerability allows attackers to weaken the security policy of the SQL Server by elevating its privileges and causing it to run in the LocalSystem security context. As a side effect, it increases the severity of the other vulnerabilities listed in this advisory and may enable attackers to compromise the server host as well.*

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function

> *This vulnerability allows remote attackers with knowledge of a valid username to execute arbitrary code with the privileges of the SQL service account.*

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

> *This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.*

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service

> *This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.*

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service

> *This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.*

III. Solution

Apply a patch from Microsoft

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function

> *Microsoft has published Security Bulletin MS02-034 to address these vulnerabilities. For more information, please see*
>
> > *http://www.microsoft.com/technet/security/bulletin/MS02-034.asp*

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

> *Microsoft has published Security Bulletin MS02-020 to address this vulnerability. For more information, please see*
>
> > *http://www.microsoft.com/technet/security/bulletin/MS02-020.asp*

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service

> *Microsoft has published Security Bulletin MS02-039 to address these vulnerabilities. For more information, please see*
>
> > *http://www.microsoft.com/technet/security/bulletin/MS02-039.asp*

Block external access to Microsoft SQL Server ports

As a workaround, it is possible to limit exposure to these vulnerabilities by restricting external access to Microsoft SQL Servers on ports 1433/tcp, 1433 /udp, 1434/tcp, and 1434/udp. Note that VU#399260 and VU#484891 can be exploited using UDP packets with forged source addresses that appear to belong to legitimate services, so system administrators should restrict all incoming packets sent to 1434/udp.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Appendix B. - CERT Vulnerability Notes sorted by Microsoft Security Bulletin ID

This appendix contains a list of CERT Vulnerability Notes sorted in reverse chronological order by their corresponding Microsoft Security Bulletin IDs. System administrators should use this list to ensure that each of the patches listed in these bulletins have been applied.

MS02-039 : Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service
VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service
VU#370308 - Microsoft SQL Server 2000 contains denial-of-service vulnerability in SQL Server Resolution Service

MS02-038 : Unchecked Buffer in SQL Server 2000 Utilities Could Allow Code Execution (Q316333)

VU#279323 - Microsoft SQL Server contains buffer overflows in several Database Consistency Checkers
VU#508387 - Microsoft SQL Server contains SQL injection vulnerability in replication stored procedures

MS02-035 : SQL Server Installation Process May Leave Passwords on System (Q263968)

VU#338195 - Microsoft SQL Server installation process leaves sensitive information on system

MS02-034 : Cumulative Patch for SQL Server (Q316333)

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function
VU#682620 - Microsoft SQL Server contains buffer overflow in code used to process "BULK INSERT" queries
VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

MS02-030 : Unchecked Buffer in SQLXML Could Lead to Code Execution (Q321911)

VU#811371 - Microsoft SQLXML ISAPI filter vulnerable to buffer overflow via *contenttype* parameter
VU#139931 - Microsoft SQLXML HTTP components vulnerable to cross-site scripting via *root* parameter

MS02-020 : SQL Extended Procedure Functions Contain Unchecked Buffers (Q319507)

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

MS02-007 : SQL Server Remote Data Source Function Contain Unchecked Buffers

VU#619707 - Microsoft SQL Server contains buffer overflows in openrowset and opendatasource
macros

MS01-060 : SQL Server Text Formatting Functions Contain Unchecked Buffers

VU#700575 - Buffer overflows in Microsoft SQL Server 7.0 and SQL Server 2000

Appendix C. - References

http://www.microsoft.com/technet/security/bulletin/MS02-007.asp
http://www.microsoft.com/technet/security/bulletin/MS02-020.asp
http://www.microsoft.com/technet/security/bulletin/MS02-030.asp
http://www.microsoft.com/technet/security/bulletin/MS02-034.asp
http://www.microsoft.com/technet/security/bulletin/MS02-035.asp
http://www.microsoft.com/technet/security/bulletin/MS02-038.asp
http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
http://www.microsoft.com/technet/security/bulletin/MS01-060.asp
http://support.microsoft.com/support/misc/kblookup.asp?id=Q316333
http://support.microsoft.com/support/misc/kblookup.asp?id=Q319507
http://support.microsoft.com/support/misc/kblookup.asp?id=Q323875
http://www.microsoft.com/technet/security/MSDEapps.asp
http://www.microsoft.com/technet/prodtechnol/sql/maintain/security/sql2ksec.asp
http://www.appsecinc.com/resources/alerts/mssql/02-0000.html
http://www.nextgenss.com/vna/ms-sql.txt
http://www.theregister.co.uk/content/4/26086.html
http://www.securityfocus.com/bid/5014
http://www.securityfocus.com/bid/5204
http://www.securityfocus.com/bid/5205
http://www.kb.cert.org/vuls/id/139931
http://www.kb.cert.org/vuls/id/225555
http://www.kb.cert.org/vuls/id/279323
http://www.kb.cert.org/vuls/id/338195
http://www.kb.cert.org/vuls/id/370308
http://www.kb.cert.org/vuls/id/399260
http://www.kb.cert.org/vuls/id/484891
http://www.kb.cert.org/vuls/id/508387
http://www.kb.cert.org/vuls/id/619707
http://www.kb.cert.org/vuls/id/627275
http://www.kb.cert.org/vuls/id/682620
http://www.kb.cert.org/vuls/id/700575
http://www.kb.cert.org/vuls/id/796313
http://www.kb.cert.org/vuls/id/811371

The CERT Coordination Center thanks NGSSoftware and Microsoft for their contributions to this document.

Author: This document was written by Jeffrey P. Lanza. Your feedback is appreciated.

Revision History

```
Jul 29, 2002:  Initial release
Jul 29, 2002:  Updated impact section for VU#484891 and VU#399260
Feb 05, 2003:  Updated systems affected and references sections to include URL for Microsoft list of MSDE
applications
```